UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,777	09/28/2001	David A. Lee	42390P11152	5083

7590   06/10/2005

BLAKELY, SOKOLOFF,
TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER
SCHUBERT, KEVIN R

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 06/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/966,777	LEE ET AL.
	Examiner	Art Unit
	Kevin Schubert	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 May 2005*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,5-9,19,20,23,25,26,28,29,32,33,35 and 36* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,5-9,19,20,23,25,26,28,29,32,33,35,36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some *   c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Claims 1-2,5-9,19-20,23,25-26,28-29,32-33, and 35-36 have been considered.

Claim Rejections - 35 USC § 112

5   The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly
claiming the subject matter which the applicant regards as his invention.

10   Claims 1-2,5-9,19-20,23,25-26,28-29,32-33, and 35-36 are rejected under 35 U.S.C. 112, second

paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter

which applicant regards as the invention.

The applicant's amended portion discloses that "valid receivers receive the recovered content key

to facilitate decryption of the content, and each of the invalid receivers receives a distinct intermediate key

15   to facilitate blocking of the content" (see amended portion of claims 1,19, and 28). However, it is not clear

whether the "distinct intermediate key" is distinct with respect to the content key or other intermediate

keys. Appropriate correction is required before the rejection is withdrawn.

Claim Rejections - 35 USC § 102

20   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for

the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public
use or on sale in this country, more than one year prior to the date of application for patent in the United
25   States.

Claims 1-2,5-9,19-20,23,25-26,28-29,32-33, and 35-36 are rejected under 35 U.S.C. 102(b) as

being anticipated by Lotspiech, U.S. Patent No. 6,118,873.

30

As per claims 1-2,5-9,19-20,23,25-26,28-29,32-33, and 35-36, the applicant discloses a method comprising the following limitations which are met by Lotspiech:

a) generating a list of update keys on a key distribution center system based on a table of secret keys identifying the valid and invalid receivers of a plurality of receivers, said list of update keys allowing

5   valid receivers to decrypt a valid content key using update keys obtained from the list of update keys (Col 5, lines 9-19);

b) generating a multiple nested list of decryption patterns based on the list of update keys (Col 2, lines 7-41);

c) broadcasting said multiple nested list of decryption patterns to the plurality of receivers (Col 2,

10   lines 7-41);

d) recovering a content key from the list of update keys by recovering a set of update keys for each receiver from the multiple nested list of decryption patterns and using the set of update keys to decrypt the content key, wherein the valid receivers receive the recovered content key to facilitate decryption of content, and each of the invalid receivers receive a distinct intermediate key to facilitate

15   blocking of the content (Col 2, lines 7-41);

Lotspiech discloses a method of broadcasting a content key to a valid receiver in which each receiver maintains a plurality of device keys and a licensing agency keeps a list which identifies the secret keys of all receivers. To broadcast a content key, a licensing agency generates a list of session numbers (update keys) which are encrypted with respective secret keys of receivers (part a). The encrypted list of

20   session numbers is combined into a session key block which is broadcast to a plurality of receivers (parts b and c). Valid receivers use their respective keys to decrypt the session numbers (update keys) which are then used to decrypt the content key. However, if an invalid receiver is identified, a compromised key of the compromised device is identified from the table of secret keys and used to encrypt a dummy number which prevents the invalid receiver from arriving at the content key and instead makes him arrive

25   at a distinct second key.

Claims 1-2,7-9,19-20,23,25-26,28-29,32-33, and 35-36 are rejected under 35 U.S.C. 102(b) as

being anticipated by Richards, U.S. Patent No. 6,069,957.

As per claims 1,19, and 28, the applicant describes a method comprising the following limitations

5   which are met by Richards:

a) generating a list of update keys on a key distribution center system based on a table of secret

keys identifying valid and invalid receivers of a plurality of receivers, said list of update keys allowing valid

receivers to decrypt a valid content key using update keys obtained from the list of update keys (Col 4,

lines 52-67; Col 9, lines 12-31);

10   b) generating a multiple nested list of decryption patterns based on the list of update keys (Col 9,

lines 12-31);

c) broadcasting said multiple nested list of decryption patterns to the plurality of receivers (Col 1,

lines 25-31);

d) recovering a content key from the list of update keys by recovering a set of update keys for

15   each receiver from the multiple nested list of decryption patterns and using the set of update keys to

decrypt the content key, wherein the valid receivers receive the recovered content key to facilitate

decryption of content, and each of the invalid receivers receives a distinct intermediate key to facilitate

blocking of the content (Col 9, lines 12-31);

Regarding part a), the key distribution center maintains a list or table of all the secret customer

20   keys. The table identifies valid and invalid receivers because the valid receivers have a secret customer

key in the table and the invalid receivers are the ones that are not reflected in the table.

As per claims 2,20, and 29, the applicant describes the method of claims 1,19, and 28, which are

met by Richards (see above), with the following limitation which is also met by Richards:

25   Wherein generating a list of update keys comprises generating at least one intermediate key and

one content key (Col 9, lines 12-31);

The intermediate keys are the CUSTOMER_CODE, which is the unique secret key of the customers maintained in the table of valid receivers, and the PK. The content key is the SK.

As per claims 7 and 25, the applicant describes the method of claims 1 and 19, which are met by

5   Richards (see above), with the following limitation which is also met by Richards:

Wherein said recovering a set of update keys for each receiver from the multiple nested list of decryption patterns comprises parsing said multiple nested list of decryption patterns to locate an entry intended for a particular receiver based on detection of a predetermined test pattern included in an entry in the multiple nested list of decryption patterns (Col 9, lines 63-67);

10   The applicant discloses that "the purpose of the test pattern is to enable the receivers to locate keys intended for that receiver within the list of keys" (Applicant: page 11). The predetermined test pattern is therefore included to alert the receiver of how to decode and parse the incoming data with regard to the levels of encryption and the various keys used to encrypt the data for the receiver. Richards discloses that a header, or predetermined test pattern, alerts the receiver that the packet is a code packet

15   and tells the receiver how to handle it.

As per claims 8,26, and 35, the applicant describes the method of claims 1,19, and 28, which are met by Richards (see above), with the following limitation which is also met by Richards:

Further comprising broadcasting content encrypted with said content key (Col 9, lines 26-31).

20

As per claims 9 and 36, the applicant describes the method of claims 8 and 35, which are met by Richards (see above), with the following additional limitation which is also met by Richards:

Further comprising decrypting said content encrypted with said content key using a content key recovered from the multiple nested list of decryption patterns (Col 9, lines 26-31).

25

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set
forth in section 102 of this title, if the differences between the subject matter sought to be patented and
5   the prior art are such that the subject matter as a whole would have been obvious at the time the
invention was made to a person having ordinary skill in the art to which said subject matter pertains.
Patentability shall not be negatived by the manner in which the invention was made.

10   Claims 5-6,23, and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Richards in view of Uz, U.S. Patent No. 6,351,538.

As per claims 5,23, and 32, the applicant describes the method of claims 1,19, and 28, which are

met by Richards (see above), with the following limitation which is met by Uz:

15   Wherein said generating a multiple nested list of decryption patterns comprises encrypting an

entry of the list of update keys using a key that is a combination of a previous update key, a secret key for

a receiver associated with the entry of the list of update keys, and an index indicating a location in said

table of secret keys associated with each entry (Uz: Col 8, lines 25-31; Richards: Col 9, lines 12-31);

Richards discloses all the limitations of claims 1,10,19,28,37, and 42. Richards also discloses

20   encrypting an entry of the list of update keys using a key that is a combination of a previous update key

and a secret key for a receiver associated with the entry of the list of update keys. This is done because

the content key, SK, is an encryption of a previous update key, PK, and a secret key for a receiver

associated with the entry of the list of update keys, CUSTOMER_CODE.

Richards fails to disclose an "index indicating a location in said table of secret keys associated

25   with each entry". Uz discloses a one way broadcasting system which broadcasts key and content

information for conditional access systems, such as a pay-per-view system. Uz system also discloses the

use of maintaining key tables. Furthermore, Uz discloses the idea of transmitting an index indicating a

location in the table of secret keys which can be used to locate keys for decryption.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Uz with those of Richards and incorporate the use of an index indicating a location in a table of secret keys so that the receiver can use the index to locate secret keys for decryption.

5   As per claims 6 and 33, the applicant describes the method of claims 5 and 32, which are met by Richards (see above), with the following additional limitation which is met by Uz:

Wherein an entry in said multiple nested list of decryption patterns includes a predetermined test pattern encrypted with the secret keys for a receiver associated with the entry of the list of update keys (Col 9, lines 63-67);

10   Richards discloses all the limitations of claims 5 and 32. However Richards fails to disclose the use of encrypting the predetermined test pattern with the secret keys for a receiver. As discussed in the rejection for claim 7, the predetermined test pattern which provides decryption instructions for the receiver corresponds to the header of Richards' system which, like the predetermined test pattern, provides decryption instructions. In short, Richards' system discloses all the limitations of the above claim except

15   for the limitation of encrypting the header information.

Uz discloses a one way broadcasting system which broadcasts key and content information for conditional access systems, such as a pay-per-view system. Furthermore, Uz discloses the idea of encrypting header information (Col 6, lines 13-14).

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to

20   combine the ideas of Uz and Richards and encrypt the header of information of Richards' system because doing so would make the system more secure and less vulnerable to hackers being able to intercept the broadcast and know information about the data.

Response to Arguments

25   Applicant's arguments filed 5/9/05 have been fully considered but they are not persuasive. The applicant argues that Richards does not disclose that invalid receivers receive a distinct intermediate key to facilitate blocking of the content. The examiner disagrees. Richards discloses a system whereby a

content key is sent to a user through a unique protocol in which a key distribution center broadcasts a key

to a valid user in a message consisting of two parts. The first part is the program key (PK) which is

encrypted using a user's unique CUSTOMER_CODE key which may be for example the serial number of

the set-top box. Once decrypted by the unique CUSTOMER_CODE key, the program key (PK) is used to

5   decrypt the secret key (SK) which is then used to decrypt content. This method is useful because it

allows the key distribution center to update the secret key, which requires sending one encrypted

message, in a frequent fashion. Updating the program key, which requires a lot of bandwidth in

individually encrypting PKs according to unique CUSTOMER_CODE keys for valid users, can be done in

a less frequent fashion.

10   Only valid receivers are able to decrypt the program key (PK) and consequently the secret

content key (SK) because only valid receivers have the unique CUSTOMER_CODE key. Richards

illustrates this by pointing out that even if an invalid receiver hacked the message he would not be able to

recover the proper intermediate key (PK) (Col 10, lines 33-48). As an example, suppose a hacker

intercepted a key update message bound for a specific set-top box. The valid set-top box, with its valid

15   CUSTOMER_CODE serial number key, would decrypt the message to arrive at the proper intermediate

key (PK) which allows for the decryption of the content key, SK. The invalid set-top box, with its invalid

CUSTOMER_CODE serial number key, would decrypt the message to arrive at a different, improper key

which is not PK. When the invalid set-top box tried to use the invalid key it would not be able to recover

the secret content key encrypted in PK.

20

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth

in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from

25   the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date

of this final action and the advisory action is not mailed until after the end of the THREE-MONTH

shortened statutory period, then the shortened statutory period will expire on the date the advisory action
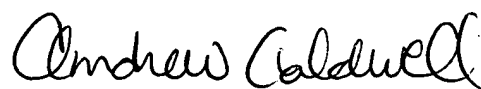
is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX

MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should

5   be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally

be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where

this application or proceeding is assigned is 703-872-9306.

10   Information regarding the status of an application may be obtained from the Patent Application

Information Retrieval (PAIR) system. Status information for published applications may be obtained from

either Private PAIR or Public PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC)

15   at 866-217-9197 (toll-free).

**ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER**

20